Version en français

Les Lumières radicales

Un monde de sources ouvertes par A.E. Freier

Les Lumières radicales - un monde de sources ouvertes (Introduction)

Nous sommes en 20XX. Les gens portent sur leur corps de petits ordinateurs très performants qui sont directement reliés à leurs organes sensoriels et donc à leur cerveau par des capteurs, des écrans et des effets sonores. Ces interfaces cérébrales sont reliées à un réseau exploité, surveillé et manipulé par un conglomérat d'entreprises technologiques géantes. En collaboration avec l'armée, les autorités pénales et une élite dirigeante corrompue des différentes régions, toutes les pensées, tous les événements, toutes les conversations et tous les mouvements des personnes sont enregistrés, analysés, manipulés et réutilisés contre elles.

De puissants réseaux neuronaux établissent le profil exact de chaque individu, lequel est ensuite transmis à des algorithmes tout aussi puissants qui dirigent les gens là où cela est prévu. La guerre, la pauvreté, les épidémies apparaissent aux individus comme un choix personnel ou du moins comme un destin inéluctable, imposé sans pitié par une grande chose sombre et inconnue. Une grande partie de la population s'est entièrement soumise à l'algorithme et à ses maîtres, défend son pouvoir, parle sa langue et salue toutes les 40 secondes environ en reliant l'interface à la tête.

La société civile, encore si puissante au siècle dernier, s'est pratiquement dissoute. La presse, les journalistes et les intellectuels (également des piliers importants d'une société libre il n'y a pas si longtemps) se soumettent ouvertement à des campagnes. La recherche de la vérité est considérée comme fausse et destructrice. La recherche de la vérité doit être empêchée. De temps en temps, certains individus ont révélé la nouvelle logique et montré qu'il ne s'agissait après tout que de l'œuvre des hommes et qu'il était possible de la changer. Tous ces individus sont désormais en prison, en fuite ou dans la folie. Tous ces individus ont été quasiment exécutés devant le public.

Les centres de pouvoir sont de plus en plus petits, mais de plus en plus puissants. 1% de la population mondiale possède tout. Le reste reçoit l'aumône. Neuf millions de personnes meurent chaque année de faim, tandis que d'autres disposent chaque jour de plusieurs millions de fois le salaire moyen d'un ouvrier. Parmi les 99% qui ne possèdent rien, une lutte sans merci pour la survie fait rage, principalement marquée par la haine et le mépris. La pensée et l'action politiques

ont cédé la place à une lutte inutile, sans danger pour les dirigeants, pour des futilités. Les préférences de consommation ou les subtilités du langage quotidien créent des camps irréconciliables qui ne peuvent jamais cesser de se battre les uns contre les autres. Et ils se battent pour RIEN, pour rien.

Une dystopie terrible, n'est-ce pas ? Comment en est-on arrivé là ? Comment avons-nous pu nous éloigner à ce point des idéaux des Lumières ? Et pouvons-nous y faire quelque chose ?

Oui, nous pouvons

Lumières radicales - un monde de sources ouvertes

La fin des Lumières ?

Aux XIXe et XXe siècles, on croyait généralement que le cours du monde et le destin des sociétés humaines évoluaient historiquement. En d'autres termes, on supposait qu'il y avait toujours une progression et que tout évoluait constamment vers le meilleur. Même dans les États bourgeois tardifs après la Seconde Guerre mondiale, on partait du principe que la prochaine génération aurait une vie plus facile. Les enfants devaient avoir une meilleure situation.

Cette idée a été déclenchée, d'une part, par l'énorme gain de connaissances que permettent les sciences de plus en plus pointues. (Dans ce contexte, il convient de mentionner Charles Darwin et sa découverte sur l'origine des espèces). Mais aussi la réflexion historique popularisée par Hegel et plus tard par Marx dans les sciences humaines.

Le savoir, l'éthique et la politique ne se sont donc pas développés par la providence divine ou les éclairs de génie éclairés de quelques élus doués, mais par un effort commun de l'humanité. Le savoir et l'expérience ont été transmis de génération en génération, remis en question, conduits sur des fausses pistes et libérés de celles-ci. L'idée était positive. Même si cette évolution était loin d'être linéaire, elle semblait être une loi et on pouvait s'attendre à un perfectionnement constant des hommes et des sociétés humaines.

L'essor toujours plus rapide de l'industrialisation, et l'accélération des connaissances en physique qui l'accompagnait, pouvaient manifestement faire des miracles. De plus en plus de tâches lourdes et désagréables étaient effectuées par des machines, le courant électrique, les véhicules autopropulsés, la transmission d'informations, d'images et de sons sur des milliers de kilomètres annonçaient un avenir glorieux.

Mais tout cela n'est pas resté sans réponse. Si tout doit être présenté de manière déterministe, empirique et calculable, alors Dieu n'existe pas. Les religions rejettent naturellement une vision historique du monde, car elles partent généralement du principe qu'il existe un premier moteur, un créateur du monde, ou du moins que tout se passe dans un cycle, un cycle. De ce point de vue, les changements ne peuvent être que superficiels et secondaires, car à la fin, tout se fond à nouveau dans l'Unique, dans l'Origine.

Il y a également eu (et il y a toujours) des forces réactionnaires. Celles-ci s'opposent à la progression, principalement pour des raisons personnelles, car elle implique la perte du pouvoir, des biens, des droits nobiliaires héréditaires ou autres. Ou bien elles veulent croire que certains groupes (les leurs) ont des droits ancestraux sur certaines terres ou même sur l'existence en général.

Les Lumières, qui constituent la base de toute société bourgeoise (et dans lesquelles d'autres modèles de société, comme le communisme, trouvent leur fondement), sont au fond un événement profondément historique et matérialiste. Aux 19e et 20e siècles, les Lumières et la Révolution française semblaient être des événements irréversibles. Mais au 21e siècle, les certitudes s'effritent.

La progression ne semble plus être une promesse de salut. La destruction de l'environnement et l'augmentation rapide des inégalités, la pauvreté fatale, la famine et la migration sont des constantes immuables de la communauté mondiale actuelle. L'avertissement(1) de Günther Anders, selon lequel l'humanité sera dépassée par sa propre révolution technologique, n'est plus depuis longtemps une intrigue bizarre pour romans de science-fiction bon marché.

Par la spécialisation et l'expertise, la numérisation, qui a changé la vie de tout le monde en très peu de temps (je pense qu'on ne se trompe pas en situant le début de la numérisation en 2000 avec la création de Google), est devenue un monstre mythique impénétrable pour l'individu isolé.

La numérisation, qui consiste à 100 % en des calculs mathématiques empiriques et rationnels, semble être devenue une idole. Arbitraire, imprévisible (!) et cruelle. Mais si elle n'est que l'œuvre de l'homme, si elle est justement calculable, ne peut-elle pas être le salut des grandes pensées des Lumières. Peut-être y aura-t-il quand même "liberté, égalité et fraternité" ? Peut-être que tout s'arrangera ?

> (1) Günther Anders *L'Obsolescence de l'homme*, t. 1 : *Sur l'âme à l'époque de la deuxième révolution industrielle*, C. H. Beck, Munich 1956

Les biens communs et le capital

L'une des principales différences entre l'époque bourgeoise et toutes celles qui l'ont précédée est le capital. Cela signifie la propriété privée de biens et d'idées communs. Les moyens de production, la terre, les brevets et, dans certaines circonstances, les hommes en tant que force de travail appartiennent à des personnes privées qui poursuivent leurs propres intérêts privés. C'est ainsi que naît la classe des capitalistes, et c'est pourquoi on appelle cette forme de société le capitalisme. L'idée libérale sous-jacente est qu'il en résulte une concurrence permanente entre les intérêts individuels et les égoïsmes, qui finissent par créer quelque chose de bon et de juste pour tous.

S'il est peut-être encore possible de penser ainsi dans un monde idéalisé et romantique d'Adam Smith, puisque tout le monde y a la même situation de départ, on s'aperçoit rapidement dans le

monde réel qu'il y a accumulation du capital. Les conditions préalables ne sont pas du tout les mêmes. Là où se trouve le capital, davantage de capital s'accumule. Des structures centralisées, des monopoles, des empires, des élites apparaissent. Le capitalisme bascule dans l'impérialisme. La violence sociale est privatisée et les autres objectifs de la révolution bourgeoise, comme l'égalité ou la démocratie, ne peuvent ainsi pas naître ou exister et deviennent impossibles. La société bourgeoise s'abolit elle-même.

Comme nous le savons au moins depuis Rosa Luxemburg (2), il ne s'agit pas d'une triste perversion à combattre, mais l'accumulation du capital et la centralisation du pouvoir sont immanentes aux sociétés basées sur la propriété privée et se produisent inévitablement.

On peut observer des dérives extrêmes dans les sociétés bourgeoises tardives de ces dernières décennies. Sous le concept de néolibéralisme développé dans les années 1940, tout est en quelque sorte privatisé. Les pensées, les sentiments, les infrastructures communales, la politique et les politiciens, la guerre et la paix. Avec l'avènement de la numérisation et sa privatisation complète, il n'y a plus aujourd'hui d'endroit qui n'appartienne à d'autres, qui ne nous soit pas complètement aliéné.

D'autre part, il y a ce que l'on appelle les Communs, un terme un peu vague (que l'on ne peut malheureusement pas traduire en français, car tout au plus pourrait-on parler de "biens communs", ce qui ne concerne toutefois que les biens). Communs désigne "ce qui appartient à tous". Le paysage en est un exemple classique. Le paysage appartient toujours à tout le monde, car même si la terre appartient à une personne en particulier, le paysage appartient toujours à celui qui le regarde.

Dans notre monde néolibéral, tous les biens communs sont peu à peu privatisés et donc, par définition, volés. L'un des exemples extrêmes est par exemple le système d'exploitation. Le système d'exploitation, c'est-à-dire le logiciel qui permet d'utiliser un ordinateur, est l'une des grandes réalisations de l'humanité, aucune entreprise, et encore moins une personne seule, ne l'a créé ou n'a le droit de le vendre.

Mais comme chacun sait, cela se fait, tout comme de nombreux autres produits, pensées et connaissances créés par l'humanité sont effrontément revendus aux hommes alors qu'ils leur appartiennent depuis longtemps.

Aussi triste que la situation puisse paraître en ce moment, elle montre aussi ouvertement comment nous pouvons la surmonter. Nous devons réussir à faire revenir le capital ou à le transférer pour la première fois dans les communs. Cette idée n'est pas nouvelle, "les moyens de production dans les mains des travailleurs". "Les maisons, appartiennent à ceux qui y vivent", etc. Cela ne peut se faire que par la force. Mais la numérisation nous ouvre une toute nouvelle possibilité. La numérisation nous ouvre une voie pour remettre les valeurs de la société et la participation à celle-ci entre les mains de ceux qui sont la société - nous, les êtres humains - ou pour la première fois.

L'idée, et elle est simple et radicale, vient du développement de logiciels. C'est l'idée des sources ouvertes, des open sources !

(2) Rosa Luxemburg - L'accumulation du capital. Une contribution à l'explication économique de l'impérialisme. Librairie Vorwärts Paul Singer, Berlin 1913

L'intelligence des masses

Dans le cadre de la progression rapide de l'industrialisation au XIXe siècle, un nouveau phénomène est apparu. Un changement sans précédent dans l'histoire de l'humanité, l'émergence des masses. Le centre de la vie culturelle et surtout économique s'est déplacé de la campagne vers la ville. D'une communauté sociale façonnée depuis des siècles dans le village ou la petite ville, on est passé aux quartiers ouvriers anonymes de masse dans les villes industrielles et les grandes villes de plus en plus gigantesques et dominantes.

Cela a fondamentalement changé la société. Les rapports de classe ont changé, passant des paysans et des seigneurs à l'armée des travailleurs, les prolétaires, et à ceux qui font travailler les travailleurs pour eux, les propriétaires d'usines et les capitalistes. La masse est donc un acteur politique. Le 20e siècle a montré que les masses peuvent jouer un rôle très ambivalent. D'une part, des guerres totales et des atrocités incroyables ont été commises au nom du peuple, de la communauté ou de son propre groupe, d'autre part, elle a mis en marche une immense démocratisation et une destruction des structures de pouvoir.

Aujourd'hui, nous vivons dans une société de masse, avec ses avantages et ses inconvénients, que nous le voulions ou non. Toute structure de domination doit, si elle veut maintenir les dirigeants au pouvoir, contrôler les masses. Outre la violence directe ou la dépendance matérielle, cela se fait principalement par le biais des médias. Si la radio jouait déjà un rôle non négligeable dans la mobilisation des gens pendant la Seconde Guerre mondiale, la télévision et, dans une mesure décisive, Internet s'y ajoutent aujourd'hui.

Internet (au sens large) est aujourd'hui l'acteur le plus important lorsqu'il s'agit de prendre une décision ou d'être incité à en prendre une. Il peut inciter les gens à aimer certains produits et marques ou à détester certains groupes, il décide de la guerre et de la paix. Ce que nous appelons aujourd'hui l'Internet est dominé par une poignée d'énormes groupes technologiques qui, s'ils le font, ne se donnent que peu de mal pour cacher leurs liens avec l'armée et le pouvoir.

A première vue, il semble aujourd'hui que l'on parvienne sans peine à diriger les gens et à les manipuler. Les masses semblent stupides et apathiques, tout au plus capables de s'unir pour former une foule. Mais si l'on y regarde de plus près, on constate un phénomène qui se produit presque toujours lors de la mise en réseau des personnes et des cultures, l'échange de connaissances, la multiplication des connaissances, l'intelligence des masses.

Combien de carreaux ont été posés et combien de chaussettes ont été tricotées, avec des vidéos d'instructions trouvées sur le web ? Combien de questions ont été posées et de projets organisés ? La combinaison des connaissances de chacun est presque infinie, du moins en ce qui concerne notre petit monde sur notre petite Terre ronde. Cette combinaison du savoir de l'humanité est incroyablement puissante et, outre la pose correcte de carreaux, elle constitue une possibilité de

véritable émancipation et d'autonomisation.

Cela ne peut pas réussir si ce savoir est entre les mains de quelques groupes mentionnés plus haut et si ceux-ci peuvent en refuser l'accès, le rendre plus difficile ou le manipuler à leur guise. Ce savoir déploie son pouvoir grâce à un accès libre et illimité pour tous les individus et à la dynamique qui en résulte, à savoir que ce savoir peut être modifié, combiné et renégocié à volonté.

Pour garantir cela, il faut des sources ouvertes. Celles-ci garantissent une disponibilité permanente et une transparence permanente sur la manière dont la source a changé et sur son origine. Les sources ouvertes sont une idée radicale.

La liberté, notre bien le plus précieux ?

Descartes, Spinoza, Rousseau et Kant, ainsi que tous les autres grands penseurs et philosophes européens des Lumières, ont un principe commun (et donc central dans la pensée des Lumières) : l'autodétermination de l'homme. L'homme a un "droit naturel", un droit humain, qui lui est pour ainsi dire donné au berceau. L'homme naît avec un libre arbitre et a donc le droit naturel de prendre ses propres décisions et de décider pour lui-même.

Kant, dans son essai "Réponse à la question : qu'est-ce que les Lumières ?"(3), résume l'idée des Lumières par "Aie le courage de te servir de ta propre raison". résume-t-il. L'idée d'indépendance vis-à-vis de l'Église, des autorités et des monarques est depuis lors un élément central de toute société moderne et bourgeoise.

Contrairement à la modernité, qui est un produit purement social et européen, les Lumières semblent être un processus d'émancipation universelle inhérent à l'humanité tout entière. La liberté n'est pas négociable. La liberté est un droit humain.

Contrairement à la liberté, l'immaturité n'est pas une loi de la nature, mais l'immaturité doit être acquise. Depuis l'Antiquité, les penseurs se demandent pourquoi il est possible que quelques-uns puissent toujours s'élever au-dessus du grand nombre et lui imposer leur volonté. Pour le grand nombre, il serait en effet facile d'envoyer promener le monarque ou le seigneur.

Outre l'apathie, c'est toujours la peur qui maintient les gens dans l'esclavage. La peur de l'inconnu, la peur de l'ennemi, des maladies, des épidémies, de Dieu ou des démons. Toutes ces peurs sont anti-Lumières, car elles visent toujours un noyau irrationnel. Les Lumières européennes ont opposé à l'irrationalisme une pensée empirique et rationnelle, qui peut décrire tous les phénomènes identifiables sur terre comme une succession de causes et d'effets. Cela signifie qu'au final, tout peut être examiné, catégorisé et donc expliqué. La peur n'y a pas sa place et ne peut faire partie que de l'expérience individuelle, mais elle n'a pas de valeur universelle.

Comme nous l'avons vu plus haut, le rationalisme est loin d'être incontesté. Mais toutes nos sociétés industrielles modernes et hautement technologiques reposent sur le fait que chaque effet a une cause.

Mais est-ce encore vrai à notre époque ? Est-il souhaitable que l'individu soit libre de ses choix ? Face aux menaces de l'époque qui s'annonce ? Face au réchauffement climatique, aux épidémies et aux conflits ingérables ? Un dualisme d'avant les Lumières, une division claire entre le bien et le mal ne sont-ils pas bien mieux adaptés au défi de l'avenir qu'un libre arbitre qui finira par nous mener à notre perte ?

Cette vision du monde est très répandue en ce début de 21e siècle. Nietzsche appelle cela, non sans raison, une morale d'esclave. Un déterminisme moral simpliste, capable d'expliquer le monde par un simple concept de bien/mal, est dans tous les cas réactionnaire. De nombreux défenseurs contemporains de ce dualisme idéologique ne se considèrent pas du tout comme faisant partie de la réaction, mais comme des précurseurs d'un avenir inconnu. Il est significatif que cette idéologie comporte un mythe du nouveau départ et de la fin de l'histoire. De manière résolument dualiste, les connaissances de l'humanité sont catégorisées comme "savoir traditionnel" et présentées comme dépassées et sans avenir. La question de savoir si les enfants allemands devraient encore lire le Faust de Goethe à l'école a déjà été posée.

Si l'on réfléchissait un instant, on remarquerait facilement que cette pensée exige la fin de la raison et ferait rougir de honte même tout idéaliste religieux irrationnel.

Pourquoi, à l'heure où le monde est confronté à d'énormes défis, l'histoire ne serait-elle plus valable ? Jésus est-il revenu ? Une prophétie maya s'est-elle réalisée ? Pourquoi l'immaturité et le conformisme devraient-ils être les garants de la résolution de changements sociaux sans précédent à l'heure actuelle ? Ou n'est-il pas d'autant plus important aujourd'hui de remettre les choses en question et de parvenir à un jugement autodéterminé ?

Grâce à Hegel, nous avons obtenu un excellent outil (bien que difficile à utiliser, il faut le reconnaître) pour décrire le monde dans ses contradictions et sa totalité déroutante. Il s'agit de la dialectique. C'est notre trésor, notre grand atout. Jamais nous ne devrions y renoncer. Surtout pas pour un dualisme techno-gnostique préhistorique à la Silicon Valley, qui nous dit très tôt par smartphone ce qui est bon ou mauvais aujourd'hui. À bas l'immaturité, vive la liberté !

"Aie le courage de te servir de ton propre esprit".

> (3) Emmanuel Kant : *Qu'est-ce que les lumières?* in : Berlinische Monatsschrift, 1784

La dialectique de la liberté

Si la liberté est donc notre bien le plus précieux et que nous ne pouvons pas y renoncer sans renoncer à notre existence en tant qu'être humain, comment la gérons-nous ? La liberté est aussi

synonyme de danger.

C'est la troublante ambivalence inhérente à la liberté. Si nous ne pouvons pas restreindre la liberté sans la perdre, mais que nous ne pouvons pas non plus, en tant qu'êtres humains, vivre sans contrat remettant la loi du plus fort à sa place et empêchant l'arbitraire et l'auto-justice, que pouvons-nous donc faire pour résoudre ce paradoxe de la liberté ?

Depuis Aristote, il existe à cet effet une méthode rationnelle et scientifique pour que l'humanité ne vive ni dans l'immaturité ni dans l'arbitraire. Il s'agit de l'éthique. Contrairement à la morale, qui est sa propre négation et qui décrit en tant qu'immoralité l'état de ce qui est autre et méprisable, l'éthique est l'étude scientifique des habitudes, des coutumes et des usages.

Les sophistes présocratiques considéraient déjà qu'il était inacceptable que l'homme, en tant qu'être rationnel et doté du libre arbitre, se laisse uniquement guider par des traditions, des conventions et des règles.

Aristote élève cela au rang de science qui nous permet d'élaborer rationnellement, empiriquement, un contrat social et de le négocier sans cesse. L'éthique présuppose que l'homme est fondamentalement doué de raison et capable de réflexion. S'il ne l'était pas, il n'aurait jamais pu quitter le domaine de la sensualité naïve et du mysticisme et serait, comme un animal, simplement livré à ses pulsions et à ses instincts.

La base de l'éthique est la vertu. Contrairement à ce qui est affirmé dans les révélations et dans les despotismes, il n'existe pas de règles transcendantes établies avant la raison humaine. Les dix commandements de Moïse contredisent toute science et sont contraires à l'éthique. Non pas dans leur contenu, car il s'agit de le négocier, mais dans leur caractère irrévocable donné par Dieu.

Les constitutions que nous attendons aujourd'hui comme base d'une société moderne et éclairée n'ont pas toutes été créées par la grâce de Dieu ou par l'éclair de génie d'un seul homme. Elles ont été obtenues et négociées au cours d'un processus historique. Notre vie commune est le résultat de ce processus éthique.

Mais qu'est-ce que cela signifie pour un monde en pleine mutation, globalisé et numérisé ? Un monde dans lequel les États-nations ne jouent plus aucun rôle (même si tout le monde s'y accroche dans la panique), dans lequel les barrières linguistiques disparaissent et où la communication en temps réel est permanente ?

Ce que l'on peut dire clairement, c'est qu'un changement radical est en train de s'opérer. Que les anciennes règles, lois et constitutions, que l'ancien contrat social doivent être renégociés. L'éthique est donc la science du moment !

Les marxistes du XIXe siècle avaient déjà tenté de créer une éthique mondiale. Ils appelaient cela l'internationalisme, un mot qui porte déjà le nationalisme dans son nom. La situation au 21e siècle est différente, les frontières arbitraires se dissolvent, une véritable communauté mondiale voit le jour.

Et pour maîtriser cela, pour développer une éthique mondiale, nous avons besoin d'outils qui nous permettent de le faire. Ceux-ci doivent être, dans le sens marxien du terme, des outils d'auto-autonomisation. Les structures numériques ne doivent pas être entre les mains d'individus, d'entreprises ou de nations. La structure doit être libre.

Les personnes intelligentes et rationnelles ont compris dès le début qu'il fallait créer une base éthique pour la numérisation. La base de l'ère de l'information et du changement numérique repose sur les logiciels. Outre les systèmes et programmes propriétaires qui dominent encore aujourd'hui, le logiciel open source a vu le jour très tôt. Un logiciel qui n'appartient à personne, qui peut être développé par tous, qui garantit une liberté totale et qui est parfaitement adapté comme outil éthique d'une nouvelle société.

Le logiciel open source n'est donc pas un phénomène technique, mais éthique, politique. Une structure pour notre avenir.

La structure du pouvoir

Qu'est-ce qui s'oppose à l'établissement d'une éthique mondiale ? Pourquoi l'humanité ne se dirige-t-elle pas vers un état dans lequel tous les êtres humains peuvent vivre en sécurité, librement et dans l'autodétermination ?

Outre la conscience qu'une telle situation est difficile, voire impossible à atteindre, et le manque de courage qui en résulte pour oser faire ce pas dans l'inconnu, ce sont en premier lieu les rapports de propriété et donc les structures du pouvoir qui s'opposent fondamentalement à un tel pas.

Au début du 21e siècle, nous vivons dans une société capitaliste tardive. Comme dans toutes les sociétés capitalistes, il existe une répartition claire des rapports de pouvoir. Il y a d'une part une classe possédante qui possède les moyens de production et qui a donc le contrôle de toutes les structures sociales comme l'État, l'armée, la police, les médias, les infrastructures, etc. D'autre part, il existe une classe sans propriété, dans le sens où les moyens de production ne lui appartiennent pas, qu'elle ne peut "travailler" que pour le bénéfice de la plus-value d'un autre et qu'elle est donc exclue du profit, du sens et du succès de son propre processus de travail.

Il existe donc, comme auparavant, une société de classes. Si l'on observe la situation mondiale, on ne peut ignorer l'armée d'esclaves et de prolétaires (c'est-à-dire de personnes à qui il ne reste rien d'autre à faire que de se reproduire). Mais même dans les sociétés industrielles prospères, la séparation entre ceux qui possèdent et ceux qui ne possèdent pas est clairement maintenue, même si elle est souvent masquée par des babioles et des privilèges.

Il est donc décisif de changer les rapports de propriété et de libérer les moyens de la production sociale des mains de quelques-uns. Les mouvements prolétariens classiques des deux derniers siècles étaient convaincus qu'il existait une sorte de droit historique, que ce pouvoir devait désormais être remis entre les mains des travailleurs.

Mais nous sommes désormais à l'aube d'une communauté mondiale entièrement numérisée. Cela signifie également que les moyens de production, qui constituaient jusqu'à présent la base des structures de pouvoir de cette société, sont également numérisés. Les conditions matérielles de

toute production (outils, machines, usines) sont désormais indissociables d'un espace virtuel. Un espace qui est théoriquement divisible à l'infini et reproductible à l'infini et qui, bien qu'il repose sur des conditions matérielles, n'est pas lui-même saisissable en tant que matière.

L'une des idées fondamentales d'une société de sources ouvertes est que l'espace virtuel est si étroitement lié au monde mécanique de la production qu'un nouvel outil est en quelque sorte créé. La partie virtuelle et numérique de l'outil domine alors la partie matérielle. Si l'on parvenait donc à placer les rapports de force dans l'espace numérique dans des contextes entièrement nouveaux, les rapports de force matériels s'en trouveraient également modifiés.

Il est essentiel que ce pouvoir ne soit pas remis entre de nouvelles mains, mais qu'il soit une source ouverte utilisable, modifiable et réutilisable par tout un chacun.

En ce qui concerne les logiciels, il existe donc la définition suivante de l'open source(4) :

- Le logiciel (c'est-à-dire le texte source) est disponible sous une forme lisible et compréhensible pour l'homme.
- Le logiciel peut être copié, distribué et utilisé à volonté.
- Le logiciel peut être modifié et distribué sous sa forme modifiée.

Appliqué à nos rapports de force réels dans un monde numérique, cela signifie que les outils du pouvoir, c'est-à-dire les moyens de production, peuvent être utilisés et modifiés par n'importe qui, dans n'importe quel but. La seule condition est que les outils modifiés puissent à leur tour être utilisés et modifiés librement. Il est évident que cette définition est un non-sens dans un monde classique et matériel. Il en va autrement si l'on part du principe que la matière et l'espace virtuel se fondent l'un dans l'autre de manière indissociable. Dans ce cas, ces trois exigences, peu spectaculaires en soi, sont des explosifs sociaux.

Pensé jusqu'au bout, ce processus promet, en raison de sa capacité de changement permanent, à la fois la liberté individuelle subjective et, en raison de la rétroaction permanente, la pleine participation au processus social en tant que tel.

> (4) Source -Wikipedia "Définition de l'initiative Open Source" - https://de.wikipedia.org/wiki/Open_Source

Forces de l'éthique

Comment une renégociation éthique et donc scientifique d'un contrat social (mondial) serait-elle alors envisageable dans un monde numérique ouvert aux sources ?

La dialectique nous apprend qu'il n'existe pas une seule vérité transcendante a priori. Une civilisation et les individus qui la composent sont marqués par des ambivalences et des expériences, des présupposés et des causalités qui se contredisent. Ils sont marqués par des

vérités qui s'excluent mutuellement. Pour résoudre ce paradoxe, l'humanité a créé dans l'Antiquité classique, comme nous l'avons montré plus haut, l'éthique en tant qu'instrument rationnel permettant de négocier sans cesse ces contradictions.

Dans le développement de logiciels open source (et seulement là), il existe un processus de fork. Créer un fork signifie faire une scission d'un programme. C'est un processus en soi simple et ennuyeux dans le contrôle de version, qui doit garantir qu'un programme de base identique puisse être retravaillé dans différentes directions indépendantes.

Ainsi, toute personne est totalement libre de copier n'importe quel programme open source et de le développer selon ses propres moyens et intérêts. Le fork permet non seulement d'utiliser les connaissances acquises jusqu'alors dans le programme original, mais aussi d'intégrer dans son propre projet les futures modifications et améliorations du programme original. Il se crée également un processus de rétroaction qui peut à son tour intégrer les innovations du fork dans le programme d'origine.

On pourrait ainsi imaginer qu'un programme de commande d'ampoules serve, dans une scission, à commander des moteurs électriques et que des forks de ce programme puissent à leur tour être utilisés en robotique ou pour l'exploitation de barrages, etc.

Ce processus à première vue technique est, à y regarder de plus près, une forme de communication extrêmement complexe et extrêmement efficace en tant que processus. Un type de communication qui joue un rôle immense dans le déroulement historique de l'histoire de l'humanité et qui, grâce à la numérisation et aux connaissances acquises dans le traitement des sources ouvertes, possède une force énorme.

Ainsi, le principe du fork, issu du développement de logiciels libres, est un outil efficace, documenté et scientifique pour représenter ce processus de communication. Associée à la numérisation, cette communication se fait en temps réel et permet ainsi une renégociation, une modification et une réadaptation permanentes sans renoncer aux caractéristiques établies et déjà négociées.

Pour établir ce puissant instrument de négociation d'une éthique future, il faut une structure qui soit totalement libre. Si l'on prend la dialectique au sérieux, il est impossible de mener à bien un tel processus sans contradictions et sans conflits. Les erreurs de jugement et les chemins de traverse font également partie de la nature humaine. Les erreurs et les conflits doivent donc être possibles et acceptés, sans pour autant mettre en péril le processus lui-même.

Avec les principes du mouvement open source mentionnés ci-dessus et l'instrument des forks et des scissions dans l'espace numérique, nous disposons déjà d'outils puissants pour maîtriser cette négociation de l'éthique.

La reconquête de la vie privée

Dans son contrat social, Kant considère que la raison est divisée en une raison privée et une raison publique. La raison privée est le type de raison que nous pouvons utiliser dans notre "office", c'est-à-dire une raison soumise à de fortes restrictions et dont le respect est nécessaire au bon

déroulement des choses. La raison publique est en revanche celle du "savant". Celle-ci devrait, selon Kant, être libre et avoir le droit de tout remettre en question et de tout dire.

Outre la raison dans le domaine public, il existe encore un domaine de la sphère privée absolue. C'est-à-dire le domaine de la famille, des amis ou de son propre moi. Dans l'Antiquité, on appelait cela l'*oikos*, la communauté domestique. Tant que ce domaine ne touche pas au public, c'est-à-dire qu'il n'enfreint pas les lois universelles, tout y est permis et se négocie dans l'*oikos* lui-même. Ce n'est pas pour rien que la sexualité et d'autres choses qui pourraient "choquer l'opinion publique" s'y trouvent.

Mais que se passe-t-il dans une société numérique où ces frontières séculaires entre ces domaines se sont pratiquement dissoutes du jour au lendemain ? Cette dissolution se produit d'une part par une auto-publication permanente en temps réel dans ce que l'on appelle les "médias sociaux". D'autre part, et de manière beaucoup plus grave, par la surveillance totale et l'enregistrement techniquement réalisables et réels de tous les événements qui se déroulent dans l'espace numérique.

Comme nous nous trouvons dans un monde entièrement numérisé, tous les domaines de la vie y trouvent également une illustration. Peu importe qu'il s'agisse de la sphère privée de l'*oikos* ou de l'observation publique d'un problème de société. Si tout est donc enregistré publiquement et, comme chacun le sait aujourd'hui(5), en permanence, cela signifie l'abolition totale de la sphère privée, du domaine privé, de l'*oikos*.

C'est fatal. Alors que la raison publique et privée doit, simplement et comme de tout temps, être renégociée, la disparition de la vie privée est une césure dans l'histoire de l'humanité et était considérée jusqu'alors comme un instrument de torture du panoptique dans les établissements pénitentiaires et les prisons.

Or, la vie privée est indissociable de la liberté sociale et individuelle ainsi que de la dignité humaine en général. La reconquête de la vie privée est donc le combat décisif à l'aube d'une numérisation tous azimuts qui ne laisse plus d'espace analogique.

Mais comment cela peut-il se faire ? Dans le domaine de la sécurité des logiciels, il existe le concept de zone militarisée et démilitarisée. On part du principe que chaque appareil et chaque programme relié au réseau mondial est (ou peut être) toujours attaqué, lu, compromis et manipulé. Tout ce qui se passe sur Internet, dans l'espace numérique, se déroule donc dans la zone militarisée et est, selon la définition, exposé à des attaques permanentes.

La réponse à la question de savoir comment établir la confidentialité dans l'espace numérique provient donc logiquement de la tradition militaire. Il s'agit de la cryptographie. Depuis le début des conflits militaires, l'humanité a essayé de modifier les messages importants de manière à ce que l'ennemi ne puisse pas les analyser.

Étant donné que, sur Internet, tout peut potentiellement être dominé par "l'ennemi" (en l'occurrence, l'ennemi de la vie privée), il est donc urgent que tout ce qui est privé, aussi inintéressant et insignifiant soit-il, soit chiffré et cryptographié. L'établissement d'une cryptographie complète du domaine privé est ainsi l'une des tâches les plus importantes de

l'humanité dans la nouvelle ère.

Outre le défi de faire prendre conscience aux gens de cette réalité et de la mettre en œuvre, l'une des plus grandes difficultés réside dans le fait que des outils cryptographiques sont nécessaires pour le cryptage et le décryptage. Ceux-ci ne peuvent pas être entre les mains d'individus ou de groupes, mais doivent être libres et disponibles en tant que source ouverte. L'outil cryptographique en lui-même ne doit donc pas contenir de secrets. Le secret du cryptage, la clé, doit être entre les mains de l'individu, tout comme une clé avec laquelle on ferme la porte de son appartement avant de s'adonner à des préférences privées.

> (5) Permanent Record (2019) Edward Snowden ISBN 9781529035650

La démocratie, le meilleur des systèmes ?

La numérisation est un phénomène mondial, elle a donc le potentiel d'établir une véritable communauté mondiale égalitaire. Aujourd'hui, il est possible de communiquer en temps réel avec presque toutes les personnes dans toutes les parties du monde. Les barrières linguistiques sont facilement franchies par des logiciels, une langue mondiale peut voir le jour, composée de toutes les langues connues, qui pourraient être totalement libres et indépendantes, et pourtant chaque être humain serait capable de comprendre sans effort la langue de tout autre être humain. Tout cela serait plus que l'internationalisme des communistes, cela rendrait possible une communauté mondiale, une société mondiale.

Ce phénomène est déjà omniprésent aujourd'hui. Il déclenche un mouvement contraire tout aussi extrême, une réaction. Partout dans le monde, on observe un retour au nationalisme. Le nationalisme en tant qu'idéologie, et c'est bien de cela qu'il s'agit ici, aboutit à la barbarie, comme nous le savons de l'histoire européenne. Les détenteurs du pouvoir réagissent au flux d'informations sans frein inhérent à la numérisation par une censure et une manipulation impuissantes des informations. (Et cela vaut également pour les États autrefois bourgeois et libéraux qui, jusque-là, maintenaient au moins un semblant de respect pour la liberté d'expression).

Aussi oppressants que soient le nationalisme, la censure et l'arbitraire, aussi forte que soit cette réaction, ces phénomènes ne pourront pas jouer de rôle à long terme dans un monde entièrement globalisé et numérisé. Ils semblent déjà impuissants et pitoyables au début de cette nouvelle évolution, mais ils n'en sont que plus dangereux.

Mais s'il est possible d'établir une communauté mondiale, à quoi pourrait ressembler un système politique à la hauteur ? Dans la politique classique (c'est-à-dire la science de la vie en commun) et dans la philosophie politique, on distingue souvent un système idéal et un système qui serait applicable dans les conditions réelles.

De l'Antiquité jusqu'au début des temps modernes, les formes de société imaginables sont typiquement représentées par un groupe de six avec trois bonnes et trois mauvaises formes. Les

bonnes sont le plus souvent la monarchie, qui est le règne d'un seul homme mais d'un homme bon, l'aristocratie, qui est le règne d'un petit nombre d'hommes mais d'hommes capables, et la polite, qui est le règne d'un grand nombre d'hommes mais d'hommes dignes. Les mauvaises formes sont majoritairement la démocratie, qui est le règne du peuple et donc des pauvres, l'oligarchie, qui est le règne de quelques riches, et la tyrannie, qui est le règne d'un despote, d'un tyran.

À l'époque moderne, le polite se transforme lentement en libéralisme, beaucoup plus complexe, ou en démocratie représentative, ce qui équivaut à un régime d'État. La démocratie classique se transforme en communisme, la dictature du prolétariat. Depuis le siècle des Lumières et l'émergence de l'individu en tant qu'acteur politique, une autre forme politique envisageable a vu le jour : l'anarchisme. Si dans l'Antiquité, l'anarchie n'était que l'absence de l'État, c'est-à-dire l'inexistence de la communauté, elle a été conçue avec l'apparition des droits de l'homme comme un droit naturel et de l'individu souverain, comme une domination de ce même individu, au bénéfice de tous.

Cicéron avait déjà reconnu qu'une domination pure des 6 formes décrites ci-dessus ne serait jamais adaptée à une société complexe et que les différentes formes évoluaient toujours, dans une tendance à la baisse, vers le pire et l'instabilité. Il proposait donc de relier toutes les formes, ce que l'on pourrait interpréter comme une forme précoce de l'approche dialectique.

Or, en politique, il n'existe pas de dualisme moral qui permette de distinguer facilement les bonnes des mauvaises formes de société. Dans une société moderne très complexe, et a fortiori dans une communauté mondiale, il y a tellement d'intérêts individuels légitimes et de situations de départ fondamentalement différentes qu'il devient impossible d'établir un système qui puisse y répondre. La seule possibilité qui existe est l'application systématique de l'approche dialectique.

Comme il est exclu que les contradictions puissent être unifiées, elles doivent être acceptées en tant que contradictions. Dans la dialectique, il y a la triple étape de la thèse, de l'antithèse et de la synthèse. Les parties contradictoires, la thèse et l'antithèse, se résolvent dans la synthèse. Comment réussir cette synthèse dans un monde hautement complexe est un défi pour l'humanité. Là aussi, et justement là, une numérisation des sources ouvertes peut nous être d'une énorme utilité. ☰ Menu

Les logiciels et les sources ouvertes

Si nous partons du principe, comme nous le faisons ici, que le monde entier et tous les domaines de la société sont ou seront numérisés, l'accent est mis sur une réalisation culturelle de l'humanité, le logiciel. Les logiciels et les langages de programmation ne sont donc plus un simple sous-produit d'une nouvelle technique, mais constituent l'épine dorsale et la base de ce nouveau monde numérisé.

Les langages de programmation sont des outils d'information artistiques dont la complexité et le contenu n'ont rien à envier aux langages évolués classiques. Tout ce que nous appelons aujourd'hui numérisation ou Internet repose sur des logiciels. Chaque application, chaque site web, chaque commande de machine, chaque commande de centrale nucléaire, bref, tout ce qui est numérique d'une manière ou d'une autre (et c'est justement tout dans une société numérique) est commandé par un logiciel, c'est-à-dire par un écrit créé par l'homme. C'est en quelque sorte de la

littérature dans un sens totalement nouveau.

Si l'on y réfléchit, il devient évident qu'il s'agit d'un instrument de pouvoir, voire de L'instrument de pouvoir d'une nouvelle ère. Les logiciels peuvent modifier, manipuler, supprimer et créer à volonté la base de la société de l'information, c'est-à-dire l'information. D'une part, c'est sa fonction, d'autre part, cela laisse énormément de place aux abus en tout genre.

La question est donc la suivante : comment faire en sorte que les gens, malgré leurs conditions et leurs capacités différentes, puissent devenir propriétaires du logiciel qu'ils utilisent et doivent utiliser ? La réponse est que ces logiciels doivent se décentraliser au point de n'appartenir finalement à personne, ou positivement, au point d'appartenir à tout le monde.

Ce principe semble plutôt abstrait et inapplicable. Mais il existe une logique étonnamment simple pour y parvenir. Et c'est, comme on peut s'y attendre, le logiciel open source. Toutes les applications à code source ouvert ne sont donc pas également émancipatrices, mais la structure qui se cache derrière est puissante et a la capacité d'atteindre cet objectif.

Au début du 21e siècle, la pertinence des structures à code source ouvert n'est pas reconnue. Les logiciels libres sont considérés comme des produits de niche, certes gratuits, mais généralement de mauvaise qualité. L'idée qui se cache derrière semble trop simple pour avoir une valeur sociale. Pourtant, si l'on regarde la définition de plus près, elle témoigne d'une force énorme.

Comme mentionné ci-dessus, il existe trois définitions de base comme conditions préalables.

D'une part, il y a la libre accessibilité. La première définition est la suivante : "Le logiciel se présente sous une forme lisible et compréhensible par l'homme". Cela signifie que toute personne maîtrisant le langage de programmation correspondant peut comprendre ce qui est écrit et le modifier sous n'importe quelle forme. Cela présuppose qu'il est indispensable pour une culture générale dans un monde numérisé de maîtriser l'un de ces "nouveaux" langages. Si tel était le cas, une transparence totale des structures définies ci-dessus comme instrument de pouvoir serait possible. Comme tout le monde ne peut pas le faire avec la même efficacité, il suffit, dans le cas d'un code source entièrement libre, qu'une quantité suffisamment importante de zoon politikon se charge de cette vérification des instruments en fonction des capacités individuelles. Comme le code source est ouvert, il peut s'agir d'un très grand groupe d'experts qui n'ont même pas besoin de se connaître pour effectuer cette tâche.

La deuxième définition est la suivante : "Le logiciel peut être copié, distribué et utilisé à volonté". Cela garantit d'une part une disponibilité permanente et d'autre part, c'est un renoncement radical à la propriété privée des logiciels. Le logiciel moderne est conçu comme une prestation de l'humanité et ne peut donc pas avoir de propriétaire. Si l'on relie cela à la première définition, le potentiel qui se cache derrière devient clair et l'on arrive à la troisième définition "Le logiciel peut être modifié et distribué sous sa forme modifiée".

Si tout le monde a un accès illimité à tous les logiciels et peut modifier ces textes sous n'importe quelle forme et les mettre à disposition de tous sans restriction, on obtient une combinaison incroyable de connaissances. Les contradictions sont également résolues de manière dialectique. Si les applications sont inutilisables et incorrectes pour un groupe, celui-ci peut apporter des

modifications à son avantage sans mettre sous tutelle le groupe qui s'en sort bien avec l'application originale.

Une synthèse dialectique, un véritable pluralisme pourrait voir le jour.

Fédéral, Décentralisé

George Orwell, l'un des penseurs les plus profonds et les plus influents du XXe siècle, décrit dans son livre emblématique "1984"(5) un monde de totalitarisme centralisé qui imprègne la totalité de la vie individuelle et communautaire. Bien qu'il s'agisse d'un roman, son livre est une analyse perspicace des sociétés de masse de la modernité tardive.

De nombreux exemples, parfois cruels, ont prouvé dans l'histoire récente qu'il ne s'agissait pas d'une pure fiction et que cela avait des conséquences fatales sur les individus, à l'intérieur comme à l'extérieur des sociétés en question. La base de ces totalitarismes, tant dans la vision d'Orwell que dans les réalisations historiques réelles, est toujours un centralisme radical. Un centralisme qui ne laisse aucune place à l'épanouissement individuel ou à un modèle de société pluraliste qui tienne compte des contradictions et des particularités d'une société de masse complexe et moderne.

Il faut donc partir du principe que toutes les sociétés confuses et aliénées ont tendance à se diriger vers le centralisme et le totalitarisme. Comme cela a été reconnu très tôt, la plupart des premières constitutions bourgeoises et libérales reposent sur une idée de fédéralisme, de décentralisation et d'individualisme.

La société numérique naissante a également cette tendance totalitaire. Aujourd'hui, quelques entreprises technologiques réunies en monopole dominent une grande partie de l'Internet, et ce dans un sens totalitaire. Non seulement toutes les plateformes numériques, et donc toutes les communications et interactions sociales qui s'y déroulent, sont sous le contrôle de ce monopole, mais les terminaux et la structure technique ne sont pas non plus, dans une large mesure, entre les mains de ceux qui doivent les utiliser.

Le fait qu'il en résulte un contrôle et une surveillance étendus au sens orwellien du terme est aujourd'hui bien prouvé et documenté et connu d'une grande partie des gens. La société numérisée se dirige ainsi vers les mêmes fatalismes que la société bourgeoise tardive. Très probablement avec les mêmes conséquences cruelles. Nous devons donc agir.

Là encore, les sources ouvertes et les logiciels libres nous fournissent des outils puissants. L'une des bases les plus remarquables de cette structure est le décentralisme. Comme décrit ci-dessus, les sources ouvertes peuvent être manipulées et modifiées à volonté par toute personne. Elles peuvent ainsi être adaptées à leurs propres besoins ou à ceux d'un groupe, sans pour autant compromettre les intérêts des autres groupes ou individus.

Cela est particulièrement évident en ce qui concerne l'interaction sociale entre les individus. Celles-ci se sont aujourd'hui déplacées en grande partie vers l'espace numérique. Ce type de

communication est particulièrement sensible et doit être protégé, car il s'agit de la sphère privée des individus qui, par définition, n'est pas destinée à être rendue publique. Il est facile de comprendre que cette protection de la vie privée n'est pas possible dans un espace numérique totalitaire et centralisé tel que nous le connaissons aujourd'hui. Dans une totalité, tout, même la communication la plus privée, est en soi public.

Le problème ne peut être résolu que par la décentralisation de la structure sous-jacente. Le mouvement open source est à l'origine de ce que l'on appelle l'Internet fédéré (souvent appelé Fediverse dans le langage courant). Dans cette fédération, on part du principe que la communication sociale dans l'espace numérique, par exemple, se limite à quelques procédures standard. Celles-ci sont définies comme des normes ouvertes et acceptées par chaque acteur du réseau fédéré. Il en résulte un degré extrêmement élevé de liberté individuelle et de confidentialité conséquente.

Prenons l'exemple de ce que l'on appelle les médias sociaux. Une grande partie de la communication privée se déroule sur les médias sociaux. Ces médias sont aujourd'hui entre les mains d'un monopole, d'un totalitarisme. Cette communication repose toutefois dans sa structure sur quelques actions normalisées. Ainsi, il y a la publication ou le post, le commentaire d'autres publications, l'affirmation ou le like, la republication des contenus des autres, ce que l'on appelle le partage ou la communication directe, le chat, etc.

Si ces actions reposaient sur des normes ouvertes et compréhensibles pour chaque acteur, il serait possible à toute instance indépendante respectant ces normes ouvertes de communiquer avec n'importe quelle autre instance respectant les mêmes normes, comme indiqué ci-dessus.

Ainsi, dans un cas extrême, il serait envisageable que chaque individu exploite une telle instance sur son propre matériel informatique en tant qu'instance privée, tout en étant capable de communiquer avec les autres instances. Comme les conditions pour exploiter des structures de ce type ne sont pas données à tout le monde, des acteurs sociaux tels que des associations, des communes, des universités, des groupes individuels ou des individus pourraient exploiter cette structure ouverte.

Comme le logiciel sous-jacent et les normes convenues sont disponibles en tant que sources ouvertes, ils peuvent également être utilisés par tous. Fédéral, décentralisé.

> (5)Nineteen Eighty-Four. Penguin, Londres, 2021, (édition originale actuelle) ISBN 978-0-24-145351-3

Cryptographie individuelle

Dans la théorie classique du contrat à la Rousseau ou Hobbes, c'est-à-dire dans le contractualisme, on part du principe qu'une société se développe à partir d'un état originel. Dans cet état originel, il n'y a pas encore de société ni de contrat, c'est un état de rationalisme amoral dans lequel chaque individu doit veiller à son propre bien-être pour survivre. C'est la constellation "tous contre tous". Si

la société naît d'un état originel, nous trouvons un état initial équitable ou, de manière plus profane, dans le doute, tout le monde peut tuer tout le monde. L'inégalité n'apparaît qu'avec la possession.

Selon cette théorie, une société est formée par un contrat, ce contrat naît de la nécessité. Maintenant, on n'est pas obligé de partager la théorie du contrat, mais elle montre bien dans quelles conditions les (nouvelles) sociétés se forment.

Aujourd'hui encore, nous sommes confrontés à une renégociation de la société. Toutefois, il ne s'agit pas d'un état originel, mais d'une transition de la société bourgeoise vers une société numérique. Il ne peut être question d'un état initial équitable, car la société accumulée, moderne tardive et en voie de disparition, est marquée par des inégalités extrêmes. Comme nous l'avons déjà montré, cette inégalité extrême se forme déjà dans la nouvelle société par l'émergence de monopoles numériques.

En revanche, l'état de rationalisme amoral (ce que Hobbes appelle "*homo homini lupus*" - l'homme est un loup pour l'homme) est facilement observable aujourd'hui. L'ensemble de l'espace numérique est un domaine "militarisé". En cas de doute, tout le monde attaque tout le monde, il n'y a pratiquement aucune région où l'on est en sécurité. Dès que l'on connecte un appareil à Internet, il est public et vulnérable. Chaque après-midi agréable, avec une tablette et une Smart TV sur le canapé, se déroule en fait avec le portefeuille ouvert et en sous-vêtements sur la place du marché.

Les monopoles hérités de la société capitaliste ne sont pas seulement des acteurs amoraux (comme tous les autres), mais ce sont des loups sur le chemin du nouveau Léviathan(6). Des loups au pouvoir énorme.

Pour parvenir à une société sans l'état de rationalisme amoral et d'inégalité monopolisée, nous avons là aussi besoin d'outils. Des outils qui ne cherchent pas à mettre fin à l'état de "tous contre tous", mais qui le reconnaissent et le rendent inoffensif dans sa structure.

Cet outil est la cryptographie. La cryptographie existe depuis que les hommes s'affrontent en tant que groupes opposés. De nombreuses guerres ont été remportées grâce au cryptage des informations de l'ennemi ou au décryptage des informations de l'adversaire. Étant donné que nous nous trouvons dans une zone "militarisée" dans l'espace numérique (et dans la société de l'information qui en résulte), le cryptage des informations personnelles et privées est essentiel pour chaque acteur et indispensable pour une vie numérique libre et autodéterminée.

Cela signifie que pour la première fois dans l'histoire de l'humanité, un droit à la cryptographie individuelle doit être conquis. Dans ce contexte, individuel signifie que le cryptage et le décryptage de ses propres informations ne peuvent être effectués que par un seul individu. Il n'y a donc pas d'instances intermédiaires. En clair, l'information n'existe que chez les acteurs individuels auxquels elle est adressée. C'est ce qu'on appelle le cryptage de bout en bout.

Comme nous nous trouvons dans la phase de transition entre la société civile et la société numérique, une lutte fait rage pour le droit à la cryptographie individuelle. Cette lutte est si acharnée et brutale que le terme de "cryptowars", c'est-à-dire de guerre cryptographique, s'est

imposé dans le langage courant.

Les adversaires de la cryptographie sont, comme on peut s'y attendre, le monopole numérique établi ainsi que les structures dépassées des sociétés bourgeoises tardives comme l'État et les exécutifs qui défendent les anciennes structures de pouvoir. La plupart du temps, cette réaction n'est pas justifiée par la conservation du pouvoir, mais par la méchanceté des hommes. L'humanité doit être surveillée, sinon elle se détruit. Dans ce contexte, le mantra sacré et la trinité sont souvent "terroristes, nazis, violeurs d'enfants" et la menace populiste selon laquelle, sans protection patriarcale, nous serions livrés sans défense à ces phénomènes pathologiques. Mais ce qui est visé, c'est une condamnation collective préalable de tous, comme instrument de pouvoir.

Comme nous l'avons montré plus haut, la cryptographie individuelle part également d'acteurs amoraux, mais montre clairement que la protection contre le rationalisme amoral des autres ne peut être que la protection de ses propres informations. De même, elle est décisive pour rompre avec les structures de pouvoir capitalistes héritées de l'ancienne époque.

> (6)Thomas Hobbes : Léviathan. Cambridge University Press, Cambridge 1996, ISBN 978-0-521-56797-8.

Cryptographie pratique

La décentralisation et la cryptographie individuelle sont des conditions essentielles pour permettre à tous les individus de vivre de manière émancipatrice et autonome dans l'espace numérique. Alors que la décentralisation de l'interaction numérique est une procédure structurelle et peut être réalisée indépendamment de l'individu par la mise à disposition des procédures et normes standard en tant que sources ouvertes, la cryptographie individuelle est également un problème individuel.

L'histoire de la cryptographie moderne (telle qu'elle est largement utilisée aujourd'hui dans l'espace numérique) est déjà relativement ancienne(7) et n'a tout d'abord pas grand-chose à voir avec la numérisation. La cryptographie moderne est un domaine spécialisé extrêmement complexe des mathématiques supérieures et requiert une énorme capacité d'abstraction et une connaissance approfondie des séries de chiffres, des codes et des procédures mathématiques.

Le savoir est donc réservé à un très petit groupe de personnes. En tenant compte de cela, l'un des critères d'une bonne méthode de cryptage n'est pas seulement la protection contre le décryptage par des tiers non autorisés, mais aussi la convivialité et la facilité d'utilisation de la méthode par des utilisateurs sans connaissances mathématiques correspondantes.

Étant donné qu'une cryptographie individuelle, un véritable cryptage de bout en bout, doit toujours être effectué par l'individu, puisqu'il ne peut y avoir d'instances intermédiaires, il s'agit d'un énorme défi pour une société numérique émancipée.

Jusqu'au développement de la cryptographie moderne au 20e siècle, toutes les méthodes de cryptage étaient réalisées selon le principe de la "sécurité par l'obscurité" (*security through obscurity*). Le procédé de cryptage en lui-même devait être obscur. Chaque participant qui voulait

prendre part à la communication cryptée devait donc connaître la procédure de décryptage. Cela signifiait également que tout tiers connaissant ce mode de cryptage pouvait décrypter tous les contenus cryptés à l'aide de ce procédé. Ce processus est donc hautement incertain et facile à compromettre. Et bien sûr, le caractère secret du procédé est en totale contradiction avec l'idée de sources ouvertes. Il est urgent que le procédé cryptographique existe en tant que source ouverte et qu'il soit vérifiable.

Au milieu du 20e siècle, une méthode basée sur l'échange de clés a ainsi vu le jour. Le secret nécessaire au chiffrement n'était donc plus le procédé en lui-même, mais reposait sur une clé secrète qui devait être connue à la fois de l'émetteur et du récepteur. Cela permettait d'une part de dévoiler le procédé et donc de permettre un examen scientifique de cette méthode et d'autre part, la compromission d'une clé ne remettait pas en cause l'ensemble du procédé.

Dans ce contexte, que ce soit pour le chiffrement mathématique ou numérique, la clé désigne généralement une chaîne de caractères longue et complexe qui ne peut être ni devinée, ni calculée à un coût raisonnable. Dans l'espace numérique, c'est donc le plus souvent simplement un fichier qui sert de secret. (bien entendu, la cryptographie moderne est bien plus complexe qu'il n'est possible de le montrer ici).

L'inconvénient de cette méthode de cryptage, également appelée cryptage symétrique, est que la clé elle-même doit être transmise au destinataire. Comme le cryptage et le décryptage utilisent la même clé, l'émetteur et le récepteur doivent également être en possession de cette clé. Si, dans l'espace analogique, il est encore concevable que la clé correspondante puisse être échangée par un messager de confiance ou lors d'une rencontre personnelle, cela est tout simplement impossible dans l'espace numérique avec des milliards de partenaires de communication potentiels.

En 1976, Whitfield Diffie et Martin Hellman ont développé une méthode de cryptage asymétrique(8). Cette méthode est parfaitement adaptée pour fournir un cryptage de bout en bout non compromis dans l'espace numérique, et ce même si les participants à la communication ne se connaissent pas. Aujourd'hui, ce principe est également la procédure standard de toute communication individuelle cryptée sur Internet.

Ce type de chiffrement repose sur l'idée que chaque participant possède deux clés. Une clé privée et digne de protection et une clé publique, connue de tous les autres. La clé publique est, comme son nom l'indique, mise à la disposition du public et ne peut alors que chiffrer. Une clé publique ne peut donc rien déchiffrer, pas même les contenus chiffrés avec la même clé.

En revanche, la clé privée, qui mérite d'être protégée, n'offre que la possibilité de décrypter. Les contenus chiffrés avec une clé publique ne peuvent donc être déchiffrés qu'avec la clé privée correspondante. Si l'on veut donc permettre une véritable cryptographie individuelle, il est nécessaire que chaque participant individuel à la communication numérique possède et gère lui-même au moins une telle paire de clés. Si la clé privée est perdue ou si des tiers non autorisés y ont accès, le contenu crypté est irrémédiablement perdu ou compromis.

Il s'agit là d'un problème auquel une société numérisée est confrontée. Si l'ensemble de la structure d'une société numérique ouverte existe sous forme de source ouverte et est donc disponible à tout moment, il est dans la nature des choses qu'un secret, ce qu'est la clé privée, ne

soit connu que de l'individu auquel les contenus privés sont adressés.

Dans l'espace analogique, il va de soi que les domaines privés, comme le domicile, sont protégés par une clé et qu'il faut y faire attention. Comme un secret tel qu'une clé ne peut pas être simplement déposé dans une structure ouverte, cette conscience devra également s'imposer dans une société numérique, pour un domaine privé numérique. D'autant plus qu'il n'y a pas de service de clés ni de pied-de-biche.

> (7) Claude Shannon : La théorie mathématique de la communication des systèmes de chiffrement. Dans : Ein - Aus : ausgewählte Schriften zur Kommunikations- und Nachrichtentheorie. 1ère édition. 1949 Brinkmann und Bose, Berlin 2000, ISBN 3-922660-68-1,

> (8) W. Diffie, M. E. Hellman : New Directions in Cryptography. In : IEEE Transactions on Information Theory. Volume 22, n° 6, 1976

Version #6
Erstellt: 10 November 2022 14:38:55 von reverend
Zuletzt aktualisiert: 20 November 2022 14:15:27 von reverend